Exhibit 1

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

OCLC, Inc., **Plaintiff,** **v.** **ANNA'S ARCHIVE, f/k/a PIRATE LIBRARY MIRROR, MARIA DOLORES ANASZTASIA MATIENZO, and JOHN DOES #1–20,** **Defendants.**	**Case No. 2:24-cv-00144-MHW-EPD** **Judge Michael H. Watson** **Magistrate Judge Elizabeth A. Preston Deavers**

DECLARATION OF CATARINA KIM

Catarina Kim declares the following pursuant to 28 U.S.C. § 1746:

1. My name is Catarina Kim. I am employed by Stroz Friedberg, an Aon company ("Aon"), a consulting firm that provides services across cyber security, digital forensics and incident response, investigations, and risk management. I am the Managing Director & Global Practice Leader for the Intelligence Group within Stroz Friedberg. Aon has been engaged by Squire Patton Boggs (US) LLP, counsel for OCLC, Inc., in the above-captioned matter.

2. I have been employed with Stroz Friedberg since January 2019. My team specializes in conducting research and analysis across open sources, public records, social media, and deep/dark web sources. In 2023, my team and I were engaged by Squire Patton Boggs to conduct attribution analysis for OCLC related to the website Anna's Archive.

3. I submit this declaration in support of OCLC's Motion to Serve Defendant Anna's Archive by Email, specifically, at the email addresses provided on Anna's Archive's main domains. I have knowledge of the facts stated herein based on my personal knowledge and my

review of the documents, files, websites, and other items referenced, as well as my oversight of the Aon team investigating this matter.

4. The individual Defendants in this matter own, operate, and/or control the pirate library known as Defendant Anna's Archive, previously the Pirate Library mirror. Anna's Archive currently utilizes at least twenty-three unique or rerouting domains or website addresses. I have reviewed these domains, the material on these domains, and investigated these domains and their likely operators.

5. Anna's Archive publicizes three main domains, annas-archive.org, annas-archive.se, and annas-archive.gs, two of which use foreign country countries—Sweden (".se") and South Georgia and the South Sandwich Islands (".gs.").

6. While Anna's Archive uses some domestic top-level hosting providers,[1] such as Cloudflare, this does not indicate that Anna's Archive is located in the United States. I understand Anna's Archive selected Cloudflare as a top-level host for the primary purpose of obscuring any physical location or other identifying information. This is consistent with a blog post published by Anna's Archive on March 19, 2023 in which Anna's Archive describes how it runs its websites and notes that it uses Cloudflare because Cloudflare resists certain types of copyright take-down requests and offers a free platform that does not require the input of any identifying information.[2] Exhibit A is a true and accurate copy of this blog post.

[1] A "host provider" is the company that provides the physical server space and data centers to house the end client's data. This also includes providing an IP address, which makes the data on the server reachable to users.
[2] https://annas-blog.org/how-to-run-a-shadow-library.html.

7. Anna's Archive uses mostly foreign hosts, registrars[3] and registrants,[4] as detailed in Exhibit B. Anna's Archive engaged registrant proxies to avoid disclosing their identifiers when registering their various domains. Entities serving as a registrant, in turn, use proxy services to protect, redact, or obfuscate registrant information and contact details in domain records. The registrant entities also use proxy servers to conceal the end user's IP address, webpage servers, and/or identity from the internet. Exhibit B is a chart identifying the domains and the origin of the hosts, registrars, and registrants for each of the identified domains.

8. Based on my research and investigation, the majority of individuals and entities associated with Anna's Archive are likely foreign, *i.e.*, located outside the United States. Anna's Archive and the individual defendants that own, operate, and/or control Anna's Archive rely heavily on foreign intermediaries to operate the sites associated with Anna's Archive. The individual defendants have also sought to conceal their identities when registering the Anna's Archive domain names, including by using proxy services, proxy servers, and a reverse-proxy servers to anonymize and conceal their personally identifying information.

9. Aon attempted to locate a physical address for Anna's Archive and the individuals behind it by reviewing Anna's Archive's known websites, domain records, and Domain Name System ("DNS") data points. Anna's Archive's domain records use privacy protection features to redact details about its registrants and their physical location. None of the domains provide registrant information such as formal business name, contact name, business address, or telephone

[3] A "registrar" is the organization accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") to sell domain names. Some host providers also offer registrar services.

[4] A "registrant" is the entity who registers a domain name.

number nor do these sites provide a "contact us" page that provides contact information that can be attributed to a real person.

10. Aon relied on commercial databases containing domain records, United States public aggregators, a Brazilian public records database, and databases that index the deep and dark web. Aon was not able to locate a physical address associated with Anna's Archive across these sources.

11. Aon also focused on researching the identities of individuals associated with Anna's Archive as administrators or contributors. The analysis included examining artifacts belonging to users interacting with GitHub and GitLab[5] pages affiliated with Anna's Archive and OCLC's WorldCat API. A majority of the likely individuals affiliated with Anna's Archive are outside the United States, including potentially in Brazil, Israel, and Germany. This investigation is ongoing.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: 1/23/2024
Date

Catarina Kim

[5] GitHub and GitLab are public, free coding or software development repositories.

Exhibit A

Anna's Blog

Updates about Anna's Archive.

How to run a shadow library: operations at Anna's Archive

annas-blog.org, 2023-03-19

I run Anna's Archive, the world's largest open-source non-profit search engine for shadow libraries, like Sci-Hub, Library Genesis, and Z-Library. Our goal is to make knowledge and culture readily accessible, and ultimately to build a community of people who together archive and preserve all the books in the world.

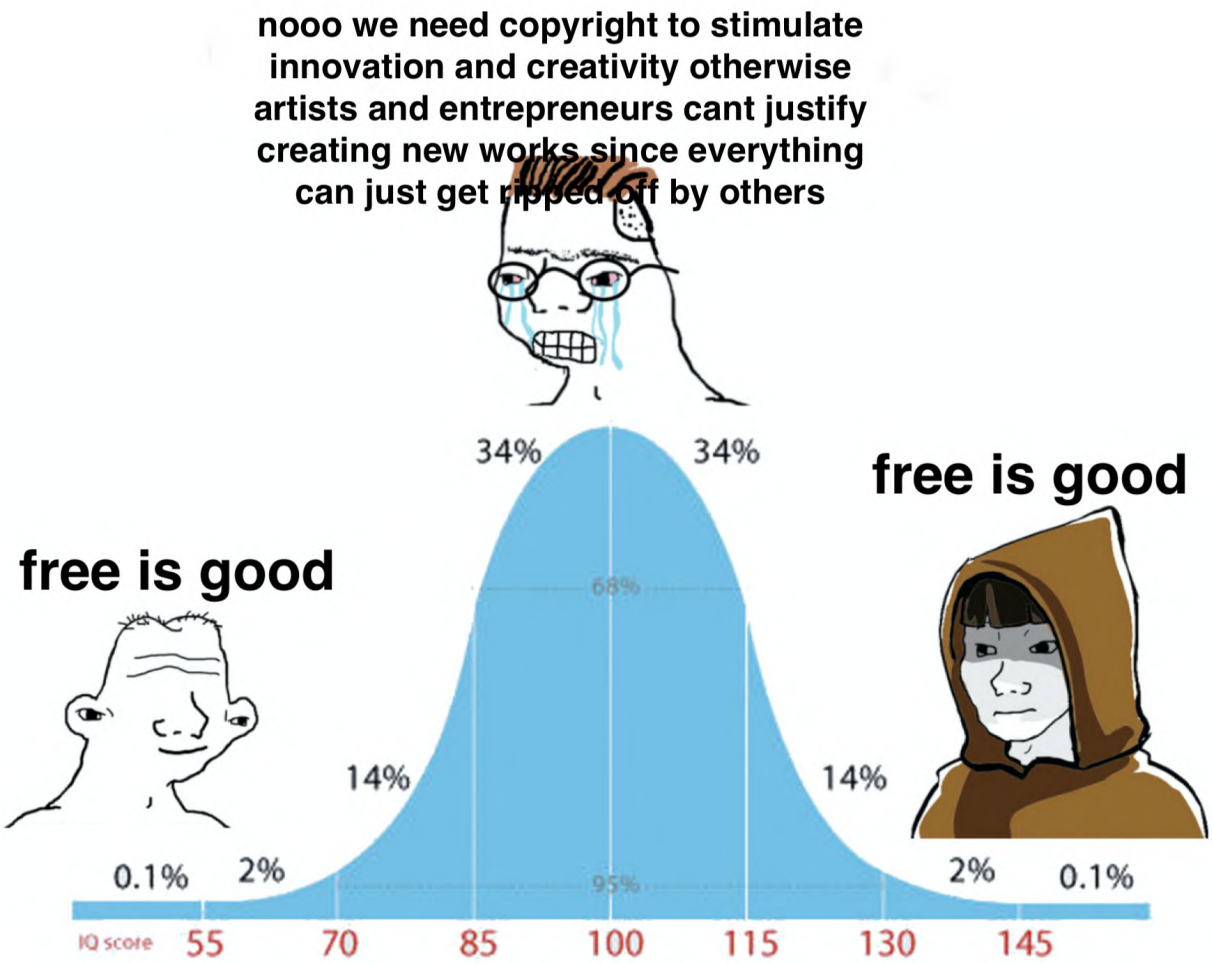
In this article I'll show how we run this website, and the unique challenges that come with operating a website with questionable legal status, since there is no "AWS for shadow charities".

Also check out the sister article How to become a pirate archivist.

Innovation tokens

Let's start with our tech stack. It is deliberately boring. We use Flask, MariaDB, and ElasticSearch. That is literally it. Search is largely a solved problem, and we don't intend to reinvent it. Besides, we have to spend our innovation tokens on something else: not being taken down by the authorities.

So how legal or illegal is Anna's Archive exactly? This mostly depends on the legal jurisdiction. Most countries believe in some form of copyright, which means that people or companies are assigned an exclusive monopoly on certain types of works for a certain period of time. As an aside, at Anna's Archive we believe while there are some benefits, overall copyright is a net-negative for society — but that is a story for another time.



This exclusive monopoly on certain works means that it is illegal for anyone outside of this monopoly to directly distribute those works — including us. But Anna's Archive is a search engine that doesn't directly distribute those works (at least not on our clearnet website), so we should be okay, right? Not exactly. In many jurisdictions it is not only illegal to distribute copyrighted works, but also to link to places that do. A classic example of this is the United States' DMCA law.

That is the strictest end of the spectrum. On the other end of the spectrum there could theoretically be countries with no copyright laws whatsoever, but these don't really exist. Pretty much every country has some form of copyright law on the books. Enforcement is a different story. There are plenty of countries with governments that do not care to enforce copyright law. There are also countries in between the two extremes, which prohibit distributing copyrighted works, but do not prohibit linking to such works.

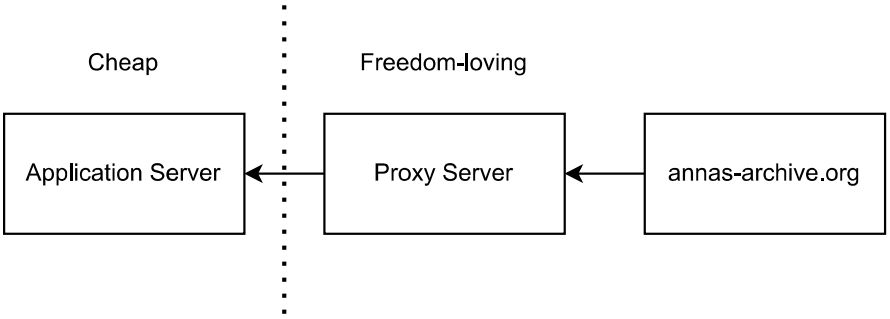
Another consideration is at the company-level. If a company operates in a jurisdiction that doesn't care about copyright, but the company itself is not willing to take any risk, then they might shut down your website as soon as anyone complains about it.

Finally, a big consideration is payments. Since we need to stay anonymous, we cannot use traditional payment methods. This leaves us with cryptocurrencies, and only a small subset of

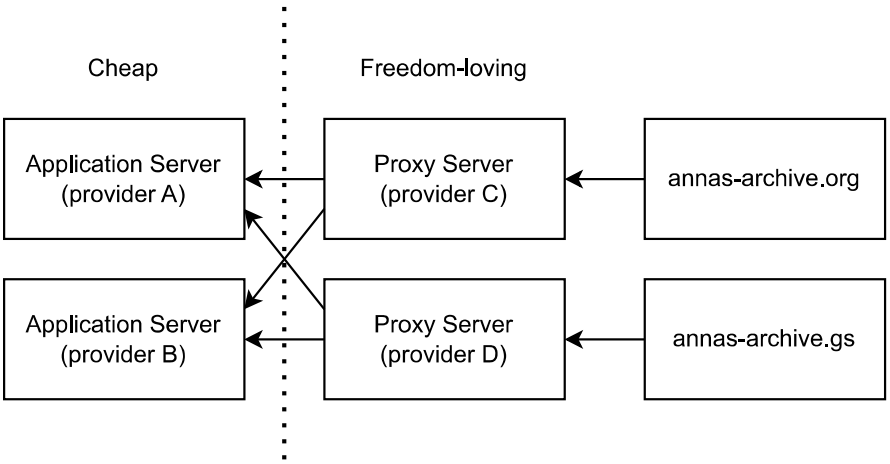
companies support those (there are virtual debit cards paid by crypto, but they are often not accepted).

System architecture

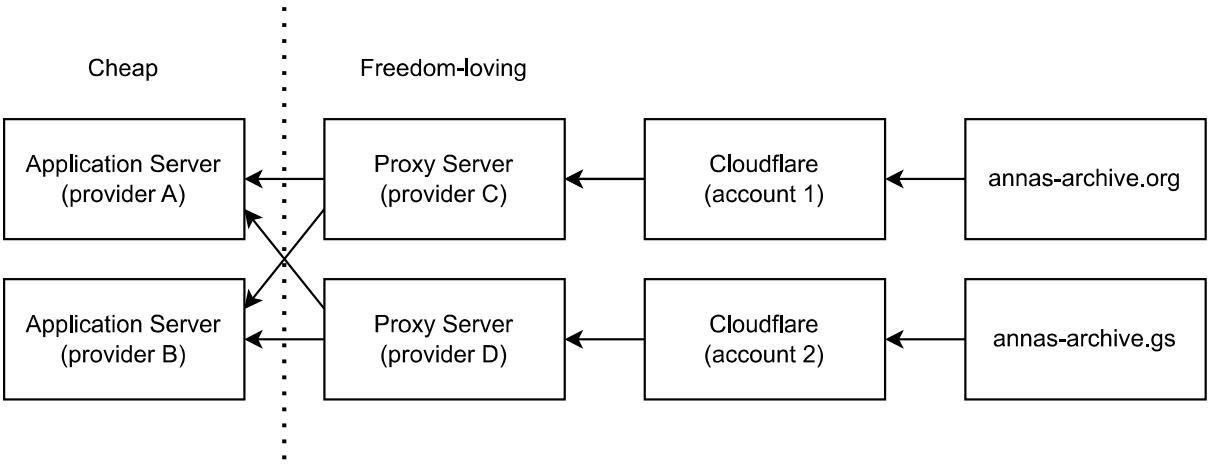
So let's say that you found some companies that are willing to host your website without shutting you down — let's call these "freedom-loving providers" . You'll quickly find that hosting everything with them is rather expensive, so you might want to find some "cheap providers" and do the actual hosting there, proxying through the freedom-loving providers. If you do it right, the cheap providers will never know what you are hosting, and never receive any complaints.



With all of these providers there is a risk of them shutting you down anyway, so you also need redundancy. We need this on all levels of our stack.

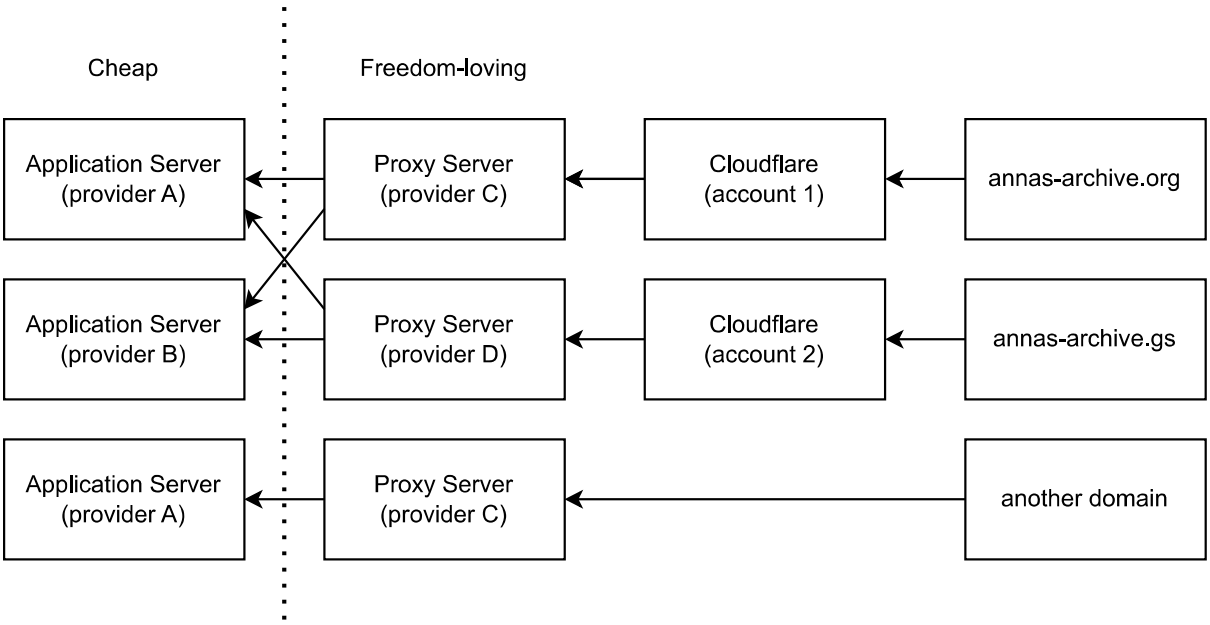


One somewhat freedom-loving company that has put itself in an interesting position is Cloudflare. They have argued that they are not a hosting provider, but a utility, like an ISP. They are therefore not subject to DMCA or other takedown requests, and forward any requests to your actual hosting provider. They have gone as far as going to court to protect this structure. We can therefore use them as another layer of caching and protection.



Cloudflare does not accept anonymous payments, so we can only use their free plan. This means that we can't use their load balancing or failover features. We therefore implemented this ourselves at the domain level. On page load, the browser will check if the current domain is still available, and if not, it rewrites all URLs to a different domain. Since Cloudflare caches many pages, this means that a user can land on our main domain, even if the proxy server is down, and then on the next click be moved over to another domain.

We still also have normal operational concerns to deal with, such as monitoring server health, logging backend and frontend errors, and so on. Our failover architecture allows for more robustness on this front as well, for example by running a completely different set of servers on one of the domains. We can even run older versions of the code and datasets on this separate domain, in case a critical bug in the main version goes unnoticed.



We can also hedge against Cloudflare turning against us, by removing it from one of the domains, such as this separate domain. Different permutations of these ideas are possible.

Tools

Let's look at what tools we use to accomplish all of this. This is very much evolving as we run into new problems and find new solutions.

- Application server: Flask, MariaDB, ElasticSearch, Docker.
- Proxy server: Varnish.
- Server management: Ansible, Checkmk, UFW.
- Development: Gitlab, Weblate, Zulip.
- Onion static hosting: Tor, Nginx.

There are some decisions that we have gone back and forth on. One is the communication between servers: we used to use Wireguard for this, but found that it occasionally stops transmitting any data, or only transmits data in one direction. This happened with several different Wireguard setups that we tried, such as wesher and wg-meshconf. We also tried tunneling ports over SSH, using autossh and sshuttle, but ran into problems there (though it is still not clear to me if autossh suffers from TCP-over-TCP issues or not — it just feels like a janky solution to me but maybe it is actually fine?).

Instead, we reverted back to direct connections between servers, hiding that a server is running on the cheap providers using IP-filtering with UFW. This has the downside that Docker doesn't work well with UFW, unless you use `network_mode: "host"`. All of this is a bit more error-prone, because you will expose your server to the internet with just a tiny misconfiguration. Perhaps we should move back to autossh — feedback would be very welcome here.

We've also gone back and forth on Varnish vs. Nginx. We currently like Varnish, but it does have its quirks and rough edges. The same applies to Checkmk: we don't love it, but it works for now. Weblate has been okay but not incredible — I sometimes fear it will lose my data whenever I try to sync it with our git repo. Flask has been good overall, but it has some weird quirks that have cost a lot of time to debug, such as configuring custom domains, or issues with its SqlAlchemy integration.

So far the other tools have been great: we have no serious complaints about MariaDB, ElasticSearch, Gitlab, Zulip, Docker, and Tor. All of these have had some issues, but nothing overly serious or time-consuming.

Conclusion

It has been an interesting experience to learn how to set up a robust and resilient shadow library search engine. There are tons more details to share in later posts, so let me know what you would like to learn more about!

As always, we're looking for donations to support this work, so be sure to check out the Donate page on Anna's Archive. We're also looking for other types of support, such as grants,

long-term sponsors, high-risk payment providers, perhaps even (tasteful!) ads. And if you want to contribute your time and skills, we're always looking for developers, translaters, and so on. Thanks for your interest and support.

- Anna and the team (Reddit, Telegram)

Exhibit B

Domain	Registrar	Registrar Location	Registrant	Registrant Location	Top-Level Hosting Provider	Host Location
annas-archive[.]gs	Sarek Oy	Finland	1337 Services LLC (Njalla)	St Kitts and Nevis	CloudFlare	California
annas-archive[.]org	Tucows	Canada	1337 Services LLC (Njalla)	St Kitts and Nevis	CloudFlare	California
annas-archive[.]se	NETIM	France	annas-archive.se	Not listed	CloudFlare	California
annas-blog[.]org	Tucows	Canada	1337 Services LLC (Njalla)	St Kitts and Nevis	CloudFlare	California
annas-software[.]org	Tucows	Canada	1337 Services LLC (Njalla)	St Kitts and Nevis	CloudFlare	California
pilimi[.]org	Tucows	Canada	1337 Services LLC (Njalla)	St Kitts and Nevis	CloudFlare	California
https://185.200.64[.]240/.	Not Listed	Not Listed	Not Listed	Not Listed	XTOM-NRT	Germany
http://84.32.231[.]244/.	Not Listed	Not Listed	Not Listed	Not Listed	Technox.com.tr	Turkey
trnet.softether[.]net	Japan Registry Services Co.	Japan	SoftEther VPN Project	Japan	Technox.com.tr	Turkey
trdir.vhealth[.]ir	Cloud DNS	Bulgaria	Not Listed	Not Listed	Technox.com.tr	Turkey
trsub.vhealth[.]ir	Cloud DNS	Bulgaria	Not Listed	Not Listed	Technox.com.tr	Turkey
http://185.145.96[.]187/	Not Listed	Not Listed	Not Listed	Not Listed	Hostwinds LLC	Washington
http://3.84.9[.]63/	Not Listed	Not Listed	Not Listed	Not Listed	Amazon Data Services NOVA	Virginia
ec2-3-84-9-63.comput-1.amazonaws[.]com	MarkMonitor Inc.	California	Amazon.com, Inc.	Washington	Amazon Data Services NOVA	Virginia
wy.xiaofankjj[.]com redirects to annas-archive[.]org	GMO Internet Group	Japan	Privacy Protection by Z.com	Japan	XTOM-NRT	Germany
cdn.xiaofankjj[.]com redirects to annas-archive[.]org	GMO Internet Group	Japan	Privacy Protection by Z.com	Japan	XTOM-NRT	Germany

test.xiaofankjj[.]com redirects to annas-archive[.]org	GMO Internet Group	Japan	Privacy Protection by Z.com	Japan	XTOM-NRT	Germany
yhy.xiaofankjj[.]com redirects to annas-archive[.]org	GMO Internet Group	Japan	Privacy Protection by Z.com	Japan	XTOM-NRT	Germany
bt.xiaofankjj.com redirects to annas-archive[.]org	GMO Internet Group	Japan	Privacy Protection by Z.com	Japan	XTOM-NRT	Germany
tr.privacypolicy.pp[.]ua redirects to annas-archive.se	ТОВ "РЕДЖЕРІ УКРАЇНА" (Regery)	Ukraine	Ali Fakoor	Iran	Technox.com.tr	Turkey
tr.sabz[.]top redirects to annas-archive[.]org	Open Provider	Netherlands	Redacted For Privacy	Iran	Technox.com.tr	Turkey
metrovp.mywire[.]org redirects to annas-archive-org	TLDS LLC dba SRSPlus.com	Not Listed	Redacted For Privacy	North Carolina	Technox.com.tr	Turkey
books.golmi[.]net redirects to annas-archive[.]org	GoDaddy	Arizona	Domains by Proxy	Arizona	Google	California